

# ISO 27001 Ready-Kit für Agenturen und KMU Zertifiziert in Rekordzeit.



# 1

## Grundlagen

Was bedeutet eine ISO 27001 Zertifizierung?

# Projektstart & Überblick

Die Vorbereitung auf eine ISO 27001 Zertifizierung ist ein anspruchsvolles Projekt, aber mit einem klaren Plan und konsequentem Vorgehen gut machbar. Wichtig ist, kontinuierlich daran zu arbeiten und ausreichend Zeit sowie die passenden Personen einzuplanen.

Mit dieser Anleitung und den Vorlagen erhalten Sie ein praxiserprobtes Fundament, um Ihr Unternehmen systematisch auf die Zertifizierung vorzubereiten.

Bevor Sie starten, bestimmen Sie eine verantwortliche Person, die das Projekt steuert – typischerweise den Informationssicherheitsbeauftragten (ISB) oder einen IT-Leiter – und binden Sie die Geschäftsführung aktiv ein. So schaffen Sie klare Rollen, Verantwortlichkeiten und einen realistischen Zeitplan.

# Was bedeutet eine ISO 27001-Zertifizierung?

## Internationale Norm für Informationssicherheit

Die ISO 27001 ist ein weltweit gültiger Standard, der beschreibt, wie Unternehmen Informationssicherheit systematisch aufbauen und steuern können. Sie definiert klare Vorgaben, um sensible Daten zuverlässig zu schützen.

## Weltweit anerkannt

Unternehmen mit einer ISO 27001-Zertifizierung zeigen, dass sie Informationssicherheit professionell umsetzen. Die Zertifizierung ist international anerkannt und stärkt das gegenseitige Vertrauen von Partnern und Kunden.

## Schutz von Vertraulichkeit, Integrität und Verfügbarkeit

Im Zentrum steht der Schutz von Daten vor unbefugtem Zugriff, Manipulation und Verlust. So wird sichergestellt, dass Informationen stets korrekt, zuverlässig und verfügbar bleiben.

## Kernbestandteile:

- Kontext der Organisation (Scope, Stakeholder)
- Führungsverantwortung (Top-Management)
- Plan-Do-Check-Act-Zyklus
- Risikobehandlung (Risk Assessment, SoA)
- Kontinuierliche Verbesserung

# Warum ISO 27001 für Agenturen und KMU?

## Agenturen arbeiten mit sensiblen Daten

Digitale Agenturen verarbeiten oft Kundeninformationen, Projektunterlagen und vertrauliche Strategien. Diese Daten sind besonders schützenswert, weil ein Verlust oder Missbrauch zu hohen Schäden führen kann.

Auch kleine und mittlere Unternehmen arbeiten heute mit sensiblen Informationen – vom Kundenprojekt bis zu Finanzdaten. Die ISO 27001 schützt diese Daten durch klare Prozesse, Verantwortlichkeiten und bewährte Sicherheitsmaßnahmen. So stärken KMU Vertrauen, vermeiden Risiken und sichern ihren langfristigen Geschäftserfolg – unabhängig von der Branche.

## Zunehmende Cyber-Bedrohungen

Angriffe durch Hacker, Schadsoftware oder Datenlecks nehmen kontinuierlich zu. Unternehmen müssen deshalb aktiv Maßnahmen ergreifen, um sich zu schützen.

## Kunden erwarten Sicherheit

Auftraggeber möchten genau sehen, wie ihre Daten geschützt werden. Eine ISO 27001-Zertifizierung bietet einen international anerkannten Nachweis dafür.

## ISO 27001 = geprüfte Sicherheit

Die Zertifizierung zeigt, dass Informationssicherheit nicht nur versprochen, sondern auch tatsächlich geprüft wurde. Das ist ein starkes Argument im Wettbewerb.

# Ziel des ISMS

Ein Informationssicherheits-Managementsystem (ISMS) ist kein einmaliges Projekt, das nach der Zertifizierung abgeschlossen ist, sondern ein **dauerhaftes Rahmenwerk**, das kontinuierlich gepflegt und weiterentwickelt werden muss.

Das Ziel eines ISMS ist es, **Informationsrisiken systematisch zu erkennen, zu bewerten und zu behandeln**, sodass sie dauerhaft auf einem akzeptablen Niveau bleiben. Gleichzeitig sorgt es dafür, dass sich das Unternehmen flexibel auf **neue Bedrohungen, technologische Entwicklungen und gesetzliche Anforderungen** reagieren kann.

Ein funktionierendes ISMS verbindet klare Prozesse, definierte Verantwortlichkeiten und regelmäßige Kontrollen. Es schafft Vertrauen zwischen Kunden, Partnern und Mitarbeitenden und erhöht gleichzeitig die **Resilienz** des Unternehmens.

Die drei zentralen Schutzziele im Überblick:

- **Vertraulichkeit:** Schutz vor unbefugtem Zugriff auf Informationen.
- **Integrität:** Stellt sicher, dass Daten und Systeme nicht unautorisiert oder unbeabsichtigt verändert werden.
- **Verfügbarkeit:** Gewährleistet, dass Informationen und Systeme stets zugänglich und funktionsfähig bleiben.



# Kernelemente der ISO 27001

## Dokumentierte Prozesse & Richtlinien

Unternehmen müssen schriftlich und transparent festlegen, wie sie mit sicherheitsrelevanten Themen umgehen – zum Beispiel mit Passwortvorgaben, Zugriffsrechten, Backups oder mobilen Endgeräten. Diese schriftlichen Regelungen bilden die Grundlage für einen sicheren Arbeitsalltag. Sie sorgen dafür, dass alle Mitarbeitenden wissen, was erlaubt ist, was nicht und wie im Ernstfall zu handeln ist.

## Risikomanagement

Ein ISMS lebt von systematischer Erfassung und Bewertung von Risiken. Typische Risiken sind Datenverlust, Cyberangriffe, Systemausfälle oder menschliche Fehler. Jedes Risiko wird hinsichtlich Eintrittswahrscheinlichkeit und möglicher Auswirkungen bewertet. Darauf aufbauend werden geeignete Maßnahmen entwickelt, die das Risiko auf ein akzeptables Niveau reduzieren – z. B. technische Schutzmaßnahmen, organisatorische Regeln oder zusätzliche Kontrollen.

## Kontinuierliche Verbesserung

Informationssicherheit ist kein einmaliges Ziel, sondern ein Prozess, der sich ständig weiterentwickelt. Durch regelmäßige interne Audits, Überprüfungen und Management-Bewertungen wird das ISMS laufend angepasst. So können neue Schwachstellen rechtzeitig erkannt und Verbesserungen geplant werden. Das Ergebnis ist ein lebendes System, das mit den Anforderungen wächst.

# Kernelemente der ISO 27001

## Einbindung aller Mitarbeiter

Ein ISMS funktioniert nur, wenn es von allen getragen wird. Informationssicherheit ist nicht Aufgabe einzelner Abteilungen, sondern ist ein fester Bestandteil der Unternehmenskultur. Schulungen, klare Rollenbeschreibungen und einfache Kommunikationswege stellen sicher, dass alle Mitarbeitenden ihren Beitrag leisten und das Sicherheitsbewusstsein gefördert wird.

## Asset Management

Im Mittelpunkt steht die Frage: *Was muss geschützt werden?* Beim Asset Management werden alle Werte (Assets) des Unternehmens erfasst – von Kundendaten und Quellcode über Server und Laptops bis hin zu Büroräumen. Diese Assets werden nach ihrer Bedeutung für Vertraulichkeit, Integrität und Verfügbarkeit bewertet und einem Verantwortlichen zugeteilt. Erst durch ein vollständiges Asset-Register ist es möglich, Risiken gezielt einzudämmen und angemessene Schutzmaßnahmen zu ergreifen.



# 2

Vorgehensweise für die Umsetzung  
eines ISMS mit ISO 27001

# Generelle Inhalte – ISO 27001 Klauseln und Annex A

- Ein Informationssicherheits-Managementsystem (ISMS) nach ISO 27001 besteht aus zwei Bausteinen: den Normkapiteln (Klauseln) und dem Anhang A (Annex A) mit den konkreten Sicherheitsmaßnahmen.
- **Normkapitel (Klauseln 4–10)**  
Diese Abschnitte beschreiben die „Management-Ebene“ des ISMS:
  - **Kontext des Unternehmens (Kap. 4):** Welche internen und externen Faktoren beeinflussen die Informationssicherheit?
  - **Führung (Kap. 5):** Welche Rolle spielt die Geschäftsleitung? Wie werden Verantwortlichkeiten festgelegt?
  - **Planung (Kap. 6):** Wie werden Risiken und Chancen systematisch ermittelt?
  - **Unterstützung (Kap. 7):** Welche Ressourcen, Kompetenzen und Schulungen sind notwendig?
  - **Betrieb (Kap. 8):** Wie setzt das Unternehmen Sicherheitsmaßnahmen um?
  - **Bewertung der Leistung (Kap. 9):** Wie wird das ISMS überwacht, gemessen und geprüft?
  - **Verbesserung (Kap. 10):** Wie geht man mit Abweichungen und Verbesserungen um?
- **Annex A (Controls / Maßnahmen)**  
Annex A enthält **93 Maßnahmen in 4 Themenbereichen** (z. B. Organisation, Menschen, IT-Systeme, Lieferanten). Sie müssen überprüfen, welche dieser Maßnahmen für Sie relevant sind und diese in einer **SoA (Statement of Applicability)** dokumentieren.

# 3

Umsetzung

# 4

## Spezielle Themen

# So nutzen Sie das Ready-Kit

## Eigene Dokumente zuordnen

Neben den Vorlagen gibt es oft bereits Dokumente in Ihrem Unternehmen, die als Nachweis dienen können.

### Vorgehen:

1. Lesen Sie das jeweilige \_info.pdf.
2. Prüfen Sie, welche Vorlagen im Kapitel enthalten sind.
3. Überlegen Sie, ob Ihr Unternehmen bereits eigene Unterlagen hat (z. B. Sicherheitsrichtlinien, Protokolle, Prozessbeschreibungen).
4. Ordnen Sie diese Dokumente den passenden Kapitelordnern zu oder verlinken Sie sie in Confluence.

# 5

Alle ISO 27001 Controls aus Anhang A im Überblick

# ISO 27001 Annex A – Grundlagen

- **93 Maßnahmen in 4 Kategorien:** Annex A umfasst 93 konkrete Sicherheitsmaßnahmen, unterteilt in organisatorische, personelle, physische und technische Bereiche
- **Risikominimierung auf allen Ebenen:** Die Maßnahmen senken systematisch das Risiko für vertrauliche Daten – von technischen bis hin zu organisatorischen und menschlichen Faktoren
- **Breites Spektrum abgedeckt:** Beispiele reichen von physischen Zugangskontrollen bis zu Verschlüsselung und Netzwerksicherheit – also alle wesentlichen Aspekte der Informationssicherheit.



# Organisatorische Maßnahmen

- **Sicherheitsleitlinien & Richtlinien:** Übergreifende IT-Sicherheitspolitik festlegen (z.B. schriftliche Sicherheitsrichtlinie) und klare Vorgaben für sichere Prozesse definieren.
- **Rollen und Zuständigkeiten:** Verantwortlichkeiten für Informationssicherheit klar zuweisen (z.B. ISO-Verantwortlicher, IT-Sicherheitsbeauftragter) und wichtige Aufgaben aufteilen (Prinzip der **Aufgabentrennung**).
- **Asset-Management & Klassifizierung:** Bestandsaufnahme aller Informationswerte durchführen und diese nach Kritikalität/Vertraulichkeit einstufen (schützt **Know-how** und sensible Daten)
- **Zugangssteuerung & Identitätsmanagement:** Zugriffsrechte nach dem **Need-to-know**-Prinzip vergeben und Nutzerkonten zentral verwalten (Passwortrichtlinien, 2-Faktor-Authentifizierung als Beispiele).
- **Lieferantenmanagement:** Sicherheitsanforderungen bei Dienstleistern und Partnern sicherstellen (z.B. Geheimhaltungsvereinbarungen, vertragliche Sicherheitsklauseln) und Risiken in der Lieferkette überwachen.
- **Vorfallsmanagement & Notfallvorsorge:** Prozesse zur Meldung und Behandlung von Sicherheitsvorfällen etablieren; Notfallpläne und **Business Continuity**-Konzepte erstellen und regelmäßig testen.
- **Compliance & Dokumentation:** Gesetzliche, regulatorische und vertragliche Anforderungen erfüllen und dies dokumentieren (Nachweise führen, regelmäßige Audits)

# Personalbezogene Maßnahmen (Personelle Sicherheit)

- **Mitarbeiterauswahl & Verträge:** Kandidaten vor Einstellung überprüfen (**Screening**) und Sicherheitsklauseln in Arbeitsverträge aufnehmen (z.B. Vertraulichkeitsvereinbarungen)
- **Schulung & Bewusstseinsbildung:** Regelmäßige Trainings zur Informationssicherheit durchführen, damit Mitarbeiter Risiken kennen und sicher handeln (**Awareness**).
- **Sichere Arbeitsumgebung:** Richtlinien für **Homeoffice/Remote Work** aufstellen (z.B. VPN-Nutzung, sichere WLAN-Regeln) und klare **Clear-Desk/Screen**-Vorgaben im Büro.
- **Onboarding/Offboarding:** Bei Eintritt Berechtigungen geordnet vergeben und beim Austritt oder internem Stellenwechsel **sofort entziehen**, um unautorisierten Zugriff zu verhindern.
- **Umgang mit Verstößen & Vorfällen:** Disziplinarische Prozesse für Sicherheitsverstöße festlegen und Meldewege definieren, damit Vorfälle sofort an die richtigen Stellen gemeldet werden

# Physische Maßnahmen (Gebäude & Umwelt)

- **Zutrittskontrollen:** Physische Sicherheitsbereiche abgrenzen (z.B. Zugang nur mit Ausweis/Schlüssel) und Besucher kontrollieren
- **Überwachung & Alarmierung:** Einsatz von Kameras, Sensoren oder Wachdienst, um unbefugten Zugang frühzeitig zu erkennen (z.B. CCTV an Eingängen, Einbruchmeldeanlagen).
- **Schutz der Infrastruktur:** Technische Einrichtungen vor Umweltgefahren schützen (z.B. Klimaanlage, Überspannungsschutz) und **Wartung** der Systeme sicherstellen
- **Sichere Arbeitsbereiche:** Sensible Zonen als “**Sicherheitsbereiche**” ausweisen, Zugänge protokollieren und Clear-Desk/Screen-Policy durchsetzen, um Informationen vor neugierigen Blicken zu schützen
- **Geräte & Datenträger:** IT-Geräte und Backup-Medien sicher aufbewahren (auch außerhalb des Firmengeländes), regelmäßige **Backups** durchführen und Datenträger sowie aussortierte Hardware sicher löschen oder zerstören.

# Technologische Maßnahmen

- **Zugriffssicherheit:** Endgeräte und Accounts absichern (z.B. Geräte-Hardening, Bildschirmsperre) und **Privilegien begrenzen** (Adminrechte nur für Berechtigte, Einsatz von MFA). Quellcodezugriffe schützen (kein unbefugter Code-Zugriff).
- **Malware-Schutz & Schwachstellenmanagement:** Virenschutz und Anti-Malware-Tools einsetzen; Systeme aktuell halten (**Patch-Management**), um bekannte Sicherheitslücken zu schließen. Unnötige oder unsichere Programme vermeiden.
- **Logging & Überwachung:** Wichtige Aktivitäten in Systemen protokollieren (**Logging**) und regelmäßig auswerten. Sicherheitsrelevante Ereignisse automatisch erkennen (**Monitoring**), um Vorfälle frühzeitig aufzudecken
- **Sicheres Konfigurations- und Änderungsmanagement:** Standard-Konfigurationen festlegen (sichere Voreinstellungen) und Änderungen an Systemen nur kontrolliert vornehmen (Change-Management-Prozess), um Stabilität und Sicherheit zu gewährleisten.
- **Datenschutz & Kryptografie:** Vertrauliche Informationen mit geeigneten Verfahren verschlüsseln (bei Speicherung und Übertragung) und Schlüssel sicher verwalten. **Datenmaskierung** einsetzen, um sensible personenbezogene Daten abzuschirmen
- **Data Leakage Prevention:** Mechanismen zum Erkennen/Verhindern von Datenabfluss einführen (z.B. Sperren von USB-Ports, Filter für vertrauliche Inhalte in E-Mails). So wird das **Risiko von Datenlecks** minimiert.
- **Backups & Redundanz:** Regelmäßige **Datensicherungen** durchführen und an getrennten Orten aufbewahren. Redundante Systeme oder Cloud-Backups vorhalten, um Ausfälle abzufangen und Geschäftsbetrieb schnell wiederherzustellen.
- **Netzwerksicherheit:** Netzwerkzugriffe absichern (Firewalls, sichere **Netzwerkdienste**) und Netzwerke segmentieren (z.B. getrennte VLANs für sensiblere Bereiche). Dadurch bleibt ein Vorfall auf einen Teil des Netzwerks begrenzt.
- **Sichere Softwareentwicklung:** Sicherheitsanforderungen in den Entwicklungsprozess integrieren (Secure Development Life Cycle). Sichere Programmierung umsetzen (Secure Coding, Code-Reviews) und Test-/Produktivumgebungen trennen, damit Schwachstellen nicht in Live-Systeme gelangen.

# Vorteile der Umsetzung (Nutzen für Unternehmen)

- **Wettbewerbsfähigkeit steigern:** ISO 27001-konforme Sicherheit bietet einen Marktvorteil und stärkt das Vertrauen von Kunden und Partnern
- **Vermeidung von Schäden:** Reduzierung des Risikos teurer Sicherheitsvorfälle, Bußgelder (z.B. bei Datenschutzverstößen) und Folgekosten.
- **Positives Image:** Verbesserung des Markenimages durch nachweislich hohe Sicherheitsstandards und verantwortungsvollen Umgang mit Daten.
- **Compliance & Audits:** Erfüllung branchenspezifischer Gesetze und Vorgaben wird erleichtert, gleichzeitig sinkt der Aufwand für Prüfungen und Audits.
- **Effiziente Prozesse:** Klar definierte Sicherheitsmaßnahmen führen zu klareren Strukturen und insgesamt effizienteren Abläufen im Unternehmen.

# 6

Nächste Schritte



**Feedback**



# Feedback

Vielen Dank & viel Erfolg!

Sie haben mit dem Ready-Kit den Grundstein gelegt, um Ihr Unternehmen erfolgreich nach **ISO 27001** zu zertifizieren. Wenn Sie sich konsequent an die Vorgaben halten und Schritt für Schritt vorgehen, wird die Zertifizierung gut gelingen.

Wir freuen uns über Ihr Feedback: Bitte melden Sie uns Fehler oder Verbesserungsvorschläge jederzeit an [feedback@iso-easy.de](mailto:feedback@iso-easy.de). Vielen Dank für Ihr Vertrauen und den Kauf des Ready-Kits von **Notivia**!

Und wenn es doch einmal hakt ...

- Falls Sie bei einzelnen Themen nicht weiterkommen: Schreiben Sie uns unter [service@iso-easy.de](mailto:service@iso-easy.de) oder rufen Sie uns an unter +49 711 35 15 705.
- Im Notfall können Sie jederzeit auf unser **Full-Service-Paket** umsteigen – der Kaufpreis des Ready-Kits wird vollständig angerechnet.
- Gerne unterstützen wir Sie auch beim **internen Audit** oder beim Finden eines geeigneten **externen Auditors**.
- Wir arbeiten erfolgreich mit unserem Partner **DQS** zusammen.



**Vielen Dank!**

Murat Aygan

Head Of Business Development & General Manager

Notivia GmbH  
Am Hohengeren 2  
70188 Stuttgart

Fon: +49 711 3838393

E-Mail: [ma@notivia.de](mailto:ma@notivia.de)

# Rechtliche Hinweise

Die in dieser Präsentation dokumentierten Gedanken und Vorschläge sind geistiges Eigentum der Notivia GmbH und unterliegen den geltenden Urhebergesetzen.

Die unautorisierte Nutzung, die ganze oder teilweise Vervielfältigung sowie jede Weitergabe an Dritte sind nicht gestattet.

Die Notivia GmbH erteilt und gewährt hinsichtlich der rechtlichen, insbesondere der wettbewerbsrechtlichen und datenschutzrechtlichen Zulässigkeit der im Rahmen der Agenturleistungen erstellten und konzipierten Inhalte, Ideen und Konzepte („Inhalte“) keine rechtliche Beratung; die Prüfung der Inhalte auf deren rechtliche Zulässigkeit, insbesondere auf deren wettbewerbsrechtliche und datenschutzrechtliche Zulässigkeit, obliegt ausschließlich dem Kunden. Folglich übernimmt die Notivia GmbH keine Haftung für die rechtliche Zulässigkeit der Inhalte, insbesondere nicht für Verstöße der Inhalte gegen wettbewerbsrechtliche und datenschutzrechtliche Bestimmungen.

Für die Übertragung der Nutzungsrechte an dieser Präsentation und der in dieser Präsentation dargestellten Inhalte, Ideen und Konzepte gelten die Regelungen der abzuschließenden Einzelverträge.